UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,004	06/14/2000	Reuben Bahar		8218

7590 12/21/2004

CAHILL, VON HELLENS & GLAZER P.L.C.
Attn: Marvin A. Glazer
155 Park One
2141 E. Highland Avenue
Phoenix, AZ 85016

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/594,004	BAHAR, REUBEN	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1,3-5, 12-14, 18-40 is/are pending in the application.

4a) Of the above claim(s) *2, 6-11, and 15-17* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,12-14 and 18-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 3-5, 12-14, and 18-40 have been examined and remains rejected due to new grounds of rejection.

2. Claims 1, 3-5, 12-14, and 18-40 are rejected under 35 U.S.C. 102(e).

3. This is a FINAL rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 3-5, 12-14, and 18-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Philyaw. (US 6,725,260).

As per claim 1:

Philyaw disclose a method of preventing piracy of a given software application comprising the steps of:

assigning a unique identification code to each authentic copy of each software application; **[col.8, lines 56-62 and col.17, lines 48-50]**

installing the software application in a data storage element on a user's computer; **[col.13, lines 54-58]**

configuring the software application to require service data to activate at least part of its functionality; **[col.27, lines 13-15]**

requiring a user to enter into the user's computer identifying data that identifies the user; **[col.12, lines 58-65 and col.14, lines 15-21]**

requiring the user to communicate user data over a communication network to a remote service system, the user data being derived, at least in part, from the unique identification code; **[col.14, lines 33-35 and col.28, lines 14-15]**

archiving user data received from the user over the communications network in a data storage element of the remote service system, said remote service system being connected to said communications network and designated to receive said user data; **[col.12, line 66 - col.13, line 24]**

comparing received user data for each unique identification code with previously archived user data corresponding to the same unique identification code to determine whether said user is pirating said software application; **[col.18, lines 37-42]**

selectively transmitting service data to the user's computer from said remote service system when said remote service system determines that said service data should be transmitted, said user's computer being connected to

said communications network and designated to storably receive said service data. **[col.13, lines 55-66 and col.28, lines 29-44]**

As per claim 3: See **col.14, lines 33-35 and col.28, lines 14-15**; discussing the unique identification code that identifies said software application installed on a data storage element of the user's computer.

As per claim 4: See **col.12, lines 58-65 and col.14, lines 15-21**; discussing user data includes identifying data that identifies the user.

As per claim 5: See **col.17, lines 49-50 and col.18, lines 49-52**; discussing user data includes product information relating to said software application installed on the data storage element of the user's computer.

As per claim 12: See **col.12, line 66 - col.13, line 24**; discussing service data is maintained in the data storage element of the remote service system.

As per claim 13: See **col.12, lines 58-65 and col.13, lines 54-58**; discussing service data comprises at least one program code sequence that activates at least part of the functionality of said software application stored on said data storage element of the user's computer.

As per claim 14: See **col.7, lines 39-40 and col.12, lines 5-6;** discussing user data includes at least one program code sequence that results in a promotional message that may be displayed to the user.

As per claim 18: See **col.12, line 66 - col.13, line 24**; discussing user data is derived at least in part from user data are stored on the data storage element of the remote service system.

As per claim 19: See **col.11, lines 46-54 and col.13, lines 38-40**; discussing selectively transmitting service data is an uploading event in which service data is automatically transferred from remote service system and storably received by the user's computer system.

As per claim 20: See **col.13, lines 38-40,62-65 and col.27, lines 34-35**; discussing selectively transmitting service data is an uploading event in which service data is manually transferred from said remote service system and storably received by the user's computer system.

As per claim 21: See **col.29, lines 24-35**; discussing selectively transmitting service data is an downloading event in which service data is made available to said user from said remote service system, and wherein said user downloads said service data into the user's computer system.

As per claim 22: See **col.13, lines 54-58 and col.27, lines 13-15**; discussing the software application includes a program code sequence that identifies the software application stored on the data storage element of the user's computer system, the software application additionally being responsive to a second program code sequence that activates at least part of the functionality of said software application, and which is transmitted to the user's computer system via said communications network.

As per claim 23:

Philyaw disclose a system for preventing piracy of a given software application, said software application having a unique identification code

associated therewith, and said software application requiring service data to activate at least part of the functionality of said software application, said system comprising:

a user computer system on which a user desires to operate the software application, said user system being connected to a communications network to transmit user data and to storably receive said service data, said user data being derived at least in part from identifying data entered by the user on the user computer system which identifies the user **[col.12, lines 58-65 and col.14, lines 15-21]**, and being derived at least in part from said unique identification code; **[col.14, lines 33-35 and col.28, lines 14-15]**

a remote service system connected to said communications network to storably user data transmitted over the communications network from the user computer system **[col.26, lines 45-62]** said remote service computer system transmitting said service data to said user computer system over said communications network when it is determined that said user is not pirating said software application. **[col.18, lines 25-43 and col.28, lines 25-60]**

As per claim 24: See **col.12, line 66 - col.13, line 24 and col.18, lines 37-43**; discussing the remote service computer system includes a data storage element for archiving user data for each unique identification code, wherein the remote service computer system compares user data received from the user computer system to user data previously archived by the remote service computer system relative to the same unique identification code, and wherein

the user data received by the remote service computer system is consistent with user data previously archived by the remote service computer system relative to the same unique identification code.

As per claim 25: See **col.12, line 66 - col.13, line 24**; discussing the service data is maintained by the remote service computer system in the data storage element used to archive the service data.

As per claim 26: See **col.12, lines 58-65 and col.13, lines 54-58**; discussing the service data consists at least in part of an activation code sequence to activate at least part of the functionality of the software application.

As per claim 27: See **col.11, lines 46-54 and col.13, lines 38-40**; discussing the service data is automatically transferred by the remote service computer system and storably received by the user computer system.

As per claim 28: See **col.13, lines 38-40,62-65 and col.27, lines 34-35**; discussing the service data manually transfers the service data from the remote service computer system to the user system.

As per claim 29: See **col.29, lines 24-35**; discussing the remote service computer system makes the service data available to the user from the remote service system, the user being able to download said service data into said user computer system.

As per claim 30: See **col.13, lines 54-58 and col.27, lines 13-15**; discussing the software application includes a program code sequence that identifies the software application stored on the data storage element of the user's computer

system, the software application additionally being responsive to a second program code sequence that activates at least part of the functionality of said software application, and which is transmitted to the user's computer system via said communications network.

As per claim 31:

Philyaw disclose a method of preventing piracy of a given software application comprising the steps of:

assigning a unique identification code to each authentic copy of each software application; **[col.8, lines 56-62 and col.17, lines 48-50]**

installing the software application in a data storage element on a user's computer; **[col.13, lines 54-58]**

configuring the software application to require service data to activate at least part of its functionality; **[col.27, lines 13-15]**

requiring a user to enter into the user's computer identifying data that identifies the user; **[col.12, lines 58-65 and col.14, lines 15-21]**

requiring the user to communicate user data over a communication network to a remote service system, the user data being derived, at least in part, from the unique identification code; **[col.14, lines 33-35 and col.28, lines 14-15]**

examining user data received by the remote service system from the user computer to determine whether the user is pirating the software application; **[col.14, lines 15-36]**

selectively transmitting service data to the user's computer from said remote service system when said remote service system determines that the user is not pirating said software application; and **[col.13, lines 55-66 and col.28, lines 29-44]**

storably receiving the transmitted service data within the data storage element of the user's computer to activate at least part of the functionality of the software application. **[col.12, lines 58-65 and col.13, lines 54-58]**

As per claim 32: See **col.12, line 66 - col.13, line 24**; discussing archiving user data received from users over the communication network in a data storage element of the remote service system.

As per claim 33: See **col.18, lines 37-42**; discussing the received user data for each unique identification code is compared with previously archived user data corresponding to the same unique identification code.

As per claim 34: See **col.7, lines 39-40 and col.12, lines 5-6;** discussing service data includes at least one program code sequence that results in a promotional message that may be displayed to the user.

As per claim 35:

Philyaw disclose a method of preventing piracy of a given software application comprising the steps of:

assigning a unique identification code to each authentic copy of each software application; **[col.8, lines 56-62 and col.17, lines 48-50]**

installing the software application in a data storage element on a user's computer; **[col.13, lines 54-58]**

configuring the software application to require service data to activate at least part of its functionality; **[col.27, lines 13-15]**

requiring the user to communicate user data over a communication network, the user data being derived, at least in part, from the identifying data that identifies the user **[col.12, lines 58-65 and col.14, lines 15-21]**, and being derived, at least in part, from the unique identification code; **[col.14, lines 33-35 and col.28, lines 14-15]**

examining user data received by the remote service system from the user computer to determine whether the user is pirating the software application; **[col.14, lines 15-36]**

selectively transmitting service data to the user's computer from said remote service system when said remote service system determines that the user is not pirating said software application; and **[col.13, lines 55-66 and col.28, lines 29-44]**

storably receiving the transmitted service data within the data storage element of the user's computer to activate at least part of the functionality of the software. **[col.12, lines 58-65 and col.13, lines 54-58]**

As per claim 36: See **col.12, line 66 - col.13, line 24**; discussing archiving user data received from users.

As per claim 37: See **col.18, lines 37-42**; discussing the received user data for each unique identification code is compared with previously archived user data corresponding to the same unique identification code.

As per claim 38:

Philyaw disclose a method of preventing piracy of a given software application comprising the steps of:

assigning a unique identification code to each authentic copy of each software application; **[col.8, lines 56-62 and col.17, lines 48-50]**

installing the software application in a data storage element on a user's computer; **[col.13, lines 54-58]**

configuring the software application to require service data, said service data being a necessary component to enable at least part of the functionality of the software application; **[col.27, lines 13-15]**

requiring the user to communicate user data over a communication network, the user data being derived, at least in part, from the identifying data that identifies the user **[col.12, lines 58-65 and col.14, lines 15-21]**, and being derived, at least in part, from the unique identification code; **[col.14, lines 33-35 and col.28, lines 14-15]**

examining user data received by the remote service system from the user computer to determine whether the user is pirating the software application; **[col.14, lines 15-36]**

selectively transmitting service data to the user's computer from said remote service system when said remote service system determines that the user is not pirating said software application; and **[col.13, lines 55-66 and col.28, lines 29-44]**

storably receiving the transmitted service data within the data storage element of the user's computer to activate at least part of the functionality of the software application. **[col.12, lines 58-65 and col.13, lines 54-58]**

As per claim 39: See **col.12, line 66 - col.13, line 24**; discussing archiving user data received from users.

As per claim 40: See **col.18, lines 37-42**; discussing the received user data for each unique identification code is compared with previously archived user data corresponding to the same unique identification code.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT
TECHNOLOGY CENTER